Remarks

The above-referenced application has been reviewed in light of the Examiner's Office Action dated January 29, 2007. The Examiner's indication of allowable subject matter is gratefully acknowledged. Claims 1-24 have been amended, and new Claims 25 and 26 have been added. Accordingly, Claims 1-26 are currently pending in this application. No new matter has been added. The Examiner's reconsideration of the rejections is respectfully requested, particularly in view of the above amendments and the following remarks.

In accordance with the Office Action, Claims 2-12 and 14-23 drew objections for informalities. Claims 2-12 and 14-23 have been amended to correct the informalities.

In accordance with the Office Action, Claim 24 stands rejected under 35 U.S.C. § 112, second paragraph. Claim 24 has been amended.

Amended Claim 24 recites, *inter alia*, "A program storage memory . . . tangibly embodying a program of instructions . . . to perform program steps for generating a simple universal hash value, the program steps comprising: inputting . . . computing . . . processing . . . and combining . . . ." Thus, amended Claim 24 currently recites a storage memory for performing said steps. Amended Claim 24 may be considered to cover a Business Method with steps comparable to those of Amended Claim 1.

In accordance with the Office Action, Claims 1-9, 11-21, 23 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicants'

Admitted Prior Art in view of U.S. Patent Application Publication 2004/0017913 by Hawkes et al. Claims 1, 13 and 24 have been amended.

Amended Claim 1 recites, *inter alia*, "A method for generating a simple universal hash value . . . comprising: inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a corresponding plurality of Ciphertext blocks; computing a Plaintext checksum value responsive to each of the plurality of Plaintext blocks; processing the plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum responsive to each of the corresponding plurality of Ciphertext blocks; and combining the Plaintext checksum and the Ciphertext checksum to obtain the simple universal hash value."

Applicants' Admitted Prior Art fairly shows inputting a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a plurality of Ciphertext blocks.

Publication number 2004/0017913 by Hawkes et al. is generally directed towards encryption with authentication. Hawkes et al. show transmitting a plurality of non-overlapping data blocks where some blocks, but not all, are enciphered, and the remainder are left in plain text. In Hawkes, checksums are only computed once for each non-overlapping portion of data. That is, Hawkes may compute a plaintext checksum for a data block or element that is to be transmitted in plaintext, and may also compute a ciphertext checksum for a data block or element that is to be transmitted in ciphertext. *See, e.g.*, Hawkes at paragraph 0068; Figure 4B, reference numerals 470 and 475 (note that Hawkes' Figure 4B, which is believed to be correct, appears to conflict with Hawkes' paragraph 0068, although such conflict is not considered relevant to the discussion at hand).

Unfortunately, neither of Hawkes plaintext and ciphertext checksums are responsive to each other. That is, altering the data in any block or element would only affect the checksum corresponding to the mode (e.g., plaintext or ciphertext) in which that block or element is transmitted. Thus, Hawkes at least fails to teach or suggest obtaining "a corresponding plurality of Ciphertext blocks" and obtaining "a Ciphertext checksum responsive to each of the corresponding plurality of Ciphertext blocks" as recited in Amended Claim 1.

In addition, Hawkes et al. actually teaches away from a plaintext checksum and a ciphertext checksum for the same block or element. Hawkes necessarily fails to produce a ciphertext checksum for blocks or elements that are not enciphered. Even more telling is that Hawkes teaches away from producing a plaintext checksum for blocks or elements that are already present in plaintext but simply not transmitted in that mode.

Amended Claims 13 and 24 each recite features similar to amended Claim 1. Accordingly, amended Claims 1, 13 and 24 are neither anticipated nor rendered obvious by Applicants' Admitted Prior Art in view of U.S. Patent Application Publication 2004/0017913 by Hawkes et al., whether taken alone or in combination with any of the other references of record in this case.

In accordance with the Office Action, Claims 10 and 22 drew objections for depending upon rejected base claims, but were indicated as comprising allowable subject matter. The Examiner's indication of allowable subject matter is gratefully acknowledged. New independent Claims 25 and 26 are submitted herewith. New Claims 25 and 26 represent the salient features of Claims 10 and 22, respectively, but have been rewritten to eliminate one or more superfluous dependencies. That is, while new Claims 25 and 26 recite the subject matter previously found in original Claims 10 and 22, respectively, and do contain all limitations of the original base claims, they do not necessarily include all limitations of the various intervening claims. No new matter has been added.

Conclusion:

Accordingly, it is respectfully submitted that amended Claims 1, 13 and 24, as well as new Claims 25 and 26, are each in condition for allowance for at least the reasons stated above. Since the remaining dependent claims each depend from one of the above claims and necessarily include each of the elements and limitations thereof, it is respectfully submitted that these claims are also in condition for allowance for at least the reasons stated, as well as for reciting additional patentable subject matter. Thus, each of Claims 1-26 is in condition for allowance. All issues raised by the Examiner having been addressed, reconsideration of the rejections and an early and favorable allowance of this case are earnestly solicited.

Respectfully submitted,

By: E. Parham 4/30/07
Eric M. Parham
Registration No. 45,747
Attorney for Applicants

Correspondence Address:

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
Telephone: (516) 692-8888
Facsimile: (516) 692-8889